

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

|                                       |                           |
|---------------------------------------|---------------------------|
| IN THE MATTER OF THE SEARCH OF        | ) Crim. No. 3:19-mj-00177 |
|                                       | )                         |
| 13720 Malaspina Street, Unit A, Eagle | ) <u>UNDER SEAL</u>       |
| River, AK 99577 and Troy Nicholas     | )                         |
| MacDermott                            | )                         |
| _____                                 | )                         |


**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Yi-Lin Lee, a Special Agent with Homeland Security Investigations (HSI),<sup>1</sup> having been first duly sworn, do hereby depose and state the following:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this Affidavit in support of an Application for a Search Warrant under Rule 41 of the Federal Rules of Criminal Procedure for 13720 Malaspina Street, Unit A, Eagle River, AK 99577 (hereinafter "SUBJECT PREMISES") and the person of Troy Nicholas MacDermott (hereinafter "MACDERMOTT"). I believe evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B), relating to material involving the sexual exploitation of minors, are located within the Subject Premises and on the person of Troy Nicholas MACDERMOTT.

<sup>1</sup> HSI is formerly Immigration and Customs Enforcement (ICE) Office of Investigations (OI).

 APR 25 2019

2. I am a SA with the United States Department of Homeland Security ("DHS"), United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), currently assigned to the Resident Agent Charge Office in Anchorage, Alaska. I have been employed in the capacity as a SA since October 2009. My duties as an HSI Agent include investigating criminal violations relating to child exploitation, narcotics trafficking, counter-proliferation, money laundering, executing and serving federal warrants and subpoenas, making warrantless arrests, and investigating violations of federal law. I have received formal training in federal laws and regulations in areas relating to immigration and customs. I have also graduated from the Criminal Investigator Training Program and the ICE Special Agent Training Program at the Federal Law Enforcement Training Center.

Previously, I served as an officer in the U.S. Coast Guard for approximately five years.

3. I am authorized by the Homeland Security Act of 2002 to perform the duties provided by law and regulation, and conduct investigations of offenses against the United States. I am further empowered to conduct investigations, request search warrants, execute search warrants, and make arrests for Title 18 crimes, including the child exploitation offenses enumerated in 18 U.S.C. § 2252 and 2252A.

4. The statements in this Affidavit are based on my personal observations, my training and experience, my investigation of this matter, and



APR 25 2019

information provided to me by other law enforcement officers. Because I make and submit this Affidavit for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, or property designed for use, intended for use, or used in committing a crime in violation of Title 18, United States Code, Sections 2252(a)(2), receipt and distribution of visual depictions of minors engaged in sexually explicit conduct, and 2252(a)(4)(B), possession of visual depictions of minors engaged in sexually explicit conduct, are located in the SUBJECT PREMISES and on the person of Troy Nicholas MACDERMOTT.

#### **STATUTORY AUTHORITY**

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252(a)(2) and (b)(1) (receipt and distribution of child pornography, and Sections 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view child pornography). Those statutes are as follows:


- (a) Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign



APR 25 2019

commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and such visual depiction is of such conduct.

(b) Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, 1 or more books, magazine, periodicals, films, video tapes, or other matter mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

//  
//  


APR 25 2019

## DEFINITIONS

6. The following terms are relevant to this affidavit in support of this application for a search warrant:

- (a) Child Erotica: The term “child erotica” means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
- (b) Child Pornography: “Child pornography” is a visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct, as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. See 18 U.S.C. §§ 2252(8).



APR 25 2019

- (c) Minor: The term “minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- (d) Sexually Explicit Conduct: The term “sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).
- (e) Visual Depictions: “Visual depiction” includes undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

7. The following technical terms are relevant to my affidavit in support of this application for a search warrant.

- (a) As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers<sup>2</sup> and other electronic devices that

---

<sup>2</sup> The term “computer” is defined by 18 U.S.C. § 1030 (e) (1) to mean “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.” This definition includes modern day cell phones, or “smart phones.”



APR 25 2019

communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including cellular networks and satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail").

(b) Set forth below are an alphabetical listing of some definitions of technical terms, used throughout this Affidavit, and in Attachments A and B, attached hereto, pertaining to the Internet and computers more generally.

- i. Bulletin Board: An Internet-based website that is either secured (accessible with a password) or unsecured, that provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content.

Bulletin boards are also referred to as "internet forums" or



APR 25 2019

“message boards.” A “post” or “posting” is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message “thread,” often labeled a “topic,” refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through “private messages.” Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

- ii. Compressed file: A “compressed file” is a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.
- iii. Computer Server (or Server): A computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and



APR 25 2019



delivers information from the server to the user's computer via the Internet.

- iv. Computer software: Digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- v. Computer-related documentation: Written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- vi. Computer system and related peripherals, and computer media: As used in this Affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras,



APR 25 2019

scanners, in addition to computer photographs, and other visual depictions of such graphic interchange formats, including but not limited to, JPG, GIF, TIF, AVI, and MPEG.

vii. Digital device: A “digital device” includes any electronic system or device capable of storing and/or processing data in digital form, including but not limited to central processing units; desktop, laptop or notebook computers, gaming systems, such as Xbox, PS3, Nintendo Wii, tablets, internet-capable cellular phones (smart phones, ; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, flash drives, thumb drives, compact disks, DVDs, and memory chips; and security devices.

viii. Domain Name: “Domain names” are common, easy to remember names associated with an internet protocol address (defined below). For example, a domain name of “www.usdoj.gov” refers to the internet protocol address of 149.101.1.32.

ix. Domain name system (DNS) server: A computer on the Internet that routes communications when a user types a



APR 25 2019

domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function. A Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DNS configuration of its configured hostnames, addresses or other information.

- x. File Transfer Protocol (FTP): A standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
- xi. Hash Function: A “hash function” is a mathematical algorithm generated against data to produce a hash value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. The term “SHA-1” or “SHA-1 hash” refers to a type of hash value that may be given to a computer file. The SHA-1 is a cryptographic hash function designed by the United States



APR 25 2019

National Security Agency and is a United States Federal Information Processing Standard. SHA stands for “secure hash algorithm.” SHA-1 hash value is the standard for unique identifying numbers. It is computationally infeasible for two files with different content to have the same hash values. I am unaware of any instance in which two files have been naturally assigned the same SHA-1 hash value.

- xii. Hyperlink: An item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- xiii. Image or copy: An “image or copy” is an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but attributes may change during the reproduction.
- xiv. Internet Service Providers (ISPs) and the Storage of ISP Records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can



APR 25 2019

offer a range of options in providing access to the Internet, including fiber optic, digital subscriber line (DSL), cable, cellular networks, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP and can access the Internet. ISPs maintain business and other records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their



APR 25 2019

computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage." See 18 U.S.C. § 2510 (15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long-term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." See 18 U.S.C. § 2711(2).

- xv. Internet Protocol Address (IP Address): Every computer or device on the Internet is referenced by a unique internet protocol address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 216.81.94.70. Each time an individual accesses the Internet,



APR 25 2019

the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Some ISP's employ dynamic IP addressing, that is they allocate any unused IP addresses at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. On the other hand, some ISP's, employ static IP addressing, that is a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. Absent some break in service, static IP addresses generally do not change over a period of time, and typically remain assigned to a specific Internet service account.

- xvi. Log files: "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff



APR 25 2019

times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a web site was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

xvii. Malicious Software (“malware”): Software designed to infiltrate a computer without the owner’s informed consent is called “malicious software” or “malware.” The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software.

xviii. Metadata: “Metadata” can be described as data about data. A photograph or image file, for example, may include metadata that describes the size, color, and resolution of the photograph. Additionally, metadata may be information about the location a photograph was taken, the date the



APR 25 2019



photograph was taken, and the make and model of the camera that was used to take the photograph.

- xix. Network Attached Storage (NAS): A file-level computer data storage server connected to a computer network providing data access to a group of clients. A NAS not only operates as a file server, but is specialized for this task either by its hardware, software, or configuration of those elements. A NAS is often a specialized computer built for storing and serving files, rather than simply a general purpose computer being used for the role.
- xx. Steganography: “Steganography” is the art and science of communicating in a way that hides the existence of the communication. Within the computer world, it can be used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.
- xxi. Structured Query Language (SQL): A special-purpose programming language designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS). SQL is used to communicate with a database. According to the American National Standards



APR 25 2019

Institute ("ANSI"), SQL is the standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database, or retrieve data from a database. Some common relational database management systems that use SQL are: Oracle, Sybase, Microsoft SQL Server, Access, Ingres, among others. SQL-DB is a log of the SQL activity.

xxii. Trace Route: A "trace route" is a network diagnostic tool used to document the list of inter-connected computers between two computers on the Internet. A trace route will list the names and IP addresses of computers that provide the physical link between two computers on the Internet. Trace routes are useful tools to help geographically identify where a computer on the Internet is physically located, and usually includes information about the registered owner of computers on the Internet.

xxiii. Uniform Resource Locator (URL): A "uniform resource locator" is the address of a resource or file located on the Internet. It is also called a "domain name."

xxiv. Web site Hosting: "Web site hosting" provides the equipment and services required to host and maintain files for one or more web sites and to provide rapid Internet connections to



APR 25 2019

those web sites. Some hosting is “shared,” which means that multiple web sites are on the same server in order to reduce associated costs. “Dedicated hosting” means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a web site. “Co-location” means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, strict humidity and temperature controls, redundant power, a dedicated Internet connection, online security, and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment as opposed to keeping it in their offices or warehouses, where the potential for fire, theft, or vandalism is greater.

xxv. The terms “*records*” and “*information*” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writings, drawings or paintings); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).



APR 25 2019

## COMPUTERS AND CHILD PORNOGRAPHY

8. Based upon my training and experience as well as my discussions with others involved in child pornography investigations, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, received and possessed.
9. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were substantial costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of this material was accomplished through a combination of personal contacts, mailings, and telephone calls. Compensation for these wares would follow the same paths. With the use of computers and the Internet, however, distributors of child pornography use distribution networks that are much faster and more cost effective. Examples of such networks include but are not limited to, personal email contacts, file-sharing services, list serves, and membership-based/subscription-based web sites. These networks also have the advantage of allowing distributors of child pornography to remain relatively anonymous.



APR 25 2019

20 Affidavit in Support of Search Warrant  
3:19-mj-00177

10. The development of computers has also revolutionized the way in which child pornography collectors interact with each other, and sexually exploit children. Computers serve four basic functions in connection with child pornography: production, communication and distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

(a) Production: Producers of child pornography can now produce high resolution images and videos directly from a common cell phone or digital camera. Today these cameras are ubiquitous, and are located on nearly every cell phone. Once taken, images and videos can be saved onto a computer, uploaded onto a website or social media platform, or attached to an email, text message, or instant message within seconds. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Videos can be edited, or spliced together to create montages of abuse that can be several minutes to several hours long. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. Additionally, the pornographer is exposed to less personal risk because this method of production does not leave an obvious trail for law enforcement to follow. In some cases,



APR 25 2019

depending upon the sophistication of the producer, it may be virtually impossible to law enforcement to determine the source of a sexually explicit image.

(b) Communication and Distribution: The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. In addition, the Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow for effortless, real time global communication. Additionally, these communications can be, relatively secure, and anonymous. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties, and verify the transportation of child pornography over the Internet is to forensically examine



APR 25 2019

22 Affidavit in Support of Search Warrant  
3:19-mj-00177

Case 3:19-mj-00177-MMS Document 1-1 Filed 04/25/19 Page 22 of 65

the recipient's computer in search of images and digital "footprints" from the websites.

(c) Storage: The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. It is not uncommon to encounter hard drives with 2 terabytes (TB) or more of data. If we assume an average image file size of 500KB, a 2 TB hard drive with approximately 1.8 TB of usable space can hold more than 3.8 million photographs. In addition, there are numerous options available for the storage of computer or digital files. To complicate matters, many individuals utilize storage options located outside the physical boundaries of a personal computer. An example of this would be a user with several thumb drives, DVDs, and/or external hard drives. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer, and can be easily concealed and carried on an individual's person.

Finally, cloud storage options allow users to save files on the



APR 25 2019

23

Affidavit in Support of Search Warrant  
3:19-mj-00177

servers of a third-party, without the need for storage on any physical device that a user might possess. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to the media storage options described above.

11. Child pornographers can now transfer photographs onto a computer directly from a digital camera, and also transfer printed child pornography to a computer with a scanner. Additionally, modern technology makes it possible to use video cameras to produce, process, and remotely save thousands of child pornography images to computer servers located in different countries. Once done, there may not be readily apparent evidence at the "scene of the crime." Only careful laboratory examination of electronic storage devices can recreate the evidence trail.
12. Collectors and distributors of child pornography can set up free, web-based accounts with multiple remote service providers that provide remote storage, e-mail services, file sharing, etc. Evidence of the remote storage of child pornography may be found on the user's computer.
13. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet providers such as Google, Microsoft, Apple, and Yahoo!, among others. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in



APR 25 2019

24

Affidavit in Support of Search Warrant

3:19-mj-00177



any variety of formats. A user can set up and access an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

14. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional. For example, a person may save an e-mail as a file or may save a favorite website in a "bookmark" type file. Information can also be retained unintentionally. For instance, traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data or intentionally "wiped" or deleted by the user.

15. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or viewed via the Internet. Even when such files have been deleted, they can often be recovered by forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.



APR 25 2019

25 Affidavit in Support of Search Warrant  
3:19-mj-00177

Case 3:19-mj-00177-MMS Document 1-1 Filed 04/25/19 Page 25 of 65

Therefore, deleted files, or remnants of deleted files, may reside for long periods of time in space on the hard drive that is not allocated to an active file. Deleted files may also reside in space that is unused after a new file has been allocated to a set block of storage space (free space or slack space). In addition, a computer's operating system may also keep a record of deleted data. Similarly, files that have been viewed in a web browser can be automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve or recover deleted files and web browser history is less dependent on when the file was downloaded or viewed than on a particular user's computer settings, storage capacity, and computer habits. In addition, individuals may maintain collections on digital devices even after those devices have outlived their useful lives, or been replaced by the user with more modern devices. I know that such devices can be stored in outbuildings, storage sheds and garages.

16. Increasingly, with faster Internet download speed and the growth of file sharing networks and other platforms through which individuals may trade child pornography, some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of



APR 25 2019

26 Affidavit in Support of Search Warrant

3:19-mj-00177

such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Furthermore, even in instances in which an individual engages in a cycle of downloading, viewing, and deleting images, a selection of favored images involving a particular child or act are often maintained on the device.

### **Kik Messenger Application**

17. The Kik Messenger application, typically referred to as "Kik", is a free chat/instant messenger social media cellular/mobile devices platform, designed and managed by Kik Interactive Incorporated, a Waterloo, Canada based company. To use this application, a user downloads the mobile messaging application via an applications service such as the Google Play Store, Apple iTunes, or other similar mobile application provider. Once downloaded and installed, the user is prompted to create an account and a username. This username will be the primary account identifier. The user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, Kik users are asked to supply a valid email address, create a password, provide an optional date of birth, and



APR 25 2019

user location. The user also has the option of uploading a “profile avatar” that is seen by other users. Once the Kik user has created an account, the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient’s username. Once another user is located or identified, Kik users can send messages, images, and videos between the two parties.

18. Kik Messenger also allows users to create chat rooms, of up to 50 people, for the purpose of communicating and exchanging images and videos. These rooms are administered by the creator who has the authority to ban and remove other users from the created room. According to Kik Messenger, more than 40% of the Kik users chat in “groups” and approximately 300,000 new groups are created every day. These groups are frequently created with a “hashtag” allowing the group or chat to be identified more easily. Once the group or chat is created Kik users have the option of sharing the “link” with all of their contacts or anyone they wish.

19. Kik Messenger users frequently advertise their Kik usernames on various social networking sites in order to meet and connect with other users. In some cases, Kik also provides various avenues, such



APR 25 2019

as dating sites and social media applications, for meeting other users. HSI undercover agents observed, in various chats, that many of the users stated they felt safe using Kik Messenger as a means of trading child pornography and for other illegal activities based on a belief that Kik's status as a Canadian business will insulate users from American criminal law and law enforcement. HSI undercover agents have noted messages posted in Kik Messenger chat rooms relating to the enforcement, deletion, or banning of users and rooms by Kik Messenger for the purpose of exchanging or distributing child pornography. HSI agents noted the comments to include the continued creation of new rooms and new user accounts to circumvent Kik Messengers enforcement efforts.

20. Kik utilizes Microsoft's PhotoDNA to match profile image hash values, against known child exploitation image has values. Anytime a positive hash value match is found, Kik's Trust and Safety team alerts the Royal Canadian Mounted Police's (RCMP) National Child Exploitation Coordination Centre (NCECC), and will provides the Subscriber data and image(s) flagged by the PhotoDNA.

**FACTS IN SUPPORT OF PROBABLE CAUSE**



APR 25 2019

21. HSI Anchorage received information from HSI Ottawa (Canada) about an individual using Kik<sup>3</sup> to distribute child exploitation material. This individual was using the Kik usernames “chrisschmidt159” and “chrissmith790”. As outlined below, investigative efforts have revealed that the likely user of “chrisschmidt159” and “chrissmith790” is Troy Nicholas MACDERMOTT.

**Kik username “chrissmith790”**

22. On December 11, 2018, at 20:40 UTC, Kik user “chrissmith790” uploaded an image in a chat room. The image was examined by Kik personnel and determined as a child pornography image. The user information was generated in a spreadsheet report as well as all activities from the opening of the account on November 22, 2018 to December 11, 2018. HSI Ottawa identified one of the IP address used, 69.178.7.183, to be administered by the General Communication Incorporated (GCI) company located in Anchorage, Alaska. HSI Ottawa forwarded the information from Kik and RCMP NCECC for the above transaction to HSI Anchorage on or about February 14, 2019.

23. Contained in the forwarded information, was the Kik IP logs for the user “chrisschmidt159.com” which show that for the period November 22, 2018

<sup>3</sup> Kik Messenger, typically referred to as “Kik”, is a free chat/ instant messenger software application for mobile devices. The Canadian company Kik Interactive produces this software. This software is available on iPhones, Android, and Windows phones.



APR 25 2019

to December 11, 2018, there were 184 logins into the Kik service. Based on the IP data, the user appears to be using IP masking technology, possibly a virtual private network (VPN) service, when logging into Kik. Using such a tool would manifest in the IP logs as logins from different locations, typically geographically distant, within a short timeframe. Due to the nature of the technology, since VPNs are often configured to be manually activated, the VPN user may not activate it (either the user forgot or for some reason chose not to), or the VPN service is disconnected due to server issues, resulting in the user's true IP being revealed. A review of "chrisschmidt159" IP logs is consistent with the use of an IP masking service. It shows IPs from various geographic countries – the U.S., Denmark, Japan, China, Mexico, Belgium, Korea, and Russia, oftentimes switching countries within minutes and hours of each other. Since a user cannot physically travel this fast, an IP masking service was most likely used. Furthermore, the IP logs show that Kik changes the remote port periodically, with it always increasing in value, in relatively tight increments. There are no instances of remote port overlaps or the port number ever decreasing or there being an unusual gap, e.g. going from a port of 55766 directly to 60000. This is consistent with there being only one installation of the Kik software logging into the service, and not multiple people geographically dispersed using the same Kik account.




APR 25 2019



24. Of the 184 IP entries, there are 34 originating from Alaska, administered by GCI Communications in Anchorage. The GCI IP addresses were the only ones that fully resolved without issues with Reverse DNS lookup, etc. so there is a high probability that they are the true IP addresses of the Kik user. The email address used for this Kik account is chrissmith790@gmail.com, and the account username as "chrissmith790".
25. On the same day, HSI Anchorage served a DHS Summons for the account that received information related to the IP address.
26. On February 22, 2019, HSI Anchorage received the Summons return from GCI. The Summons return showed Troy MACDERMOTT to be the sole account holder for the IP address service since February 2018. MACDERMOTT is a subscriber of the GCI internet service and the service address shown on the Summons return is as follow: 13720 Malaspina Street, Unit A, Eagle River, Alaska 99577.
27. On February 26, 2019, I conducted a search in Alaska Department of Public Safety's database for name matching Troy MACDERMOTT and found driver license information showing MACDERMOTT's residential address matching 13720 Malaspina Street, Unit A, Eagle River, Alaska 99577. MACDERMOTT appears to be wearing military camouflage fatigue in this driver license photo.
28. On March 8, 2019, I met with U.S. Army Criminal Investigation Division

(U.S. Army-CID) Assistant Special Agent in Charge William Stern who

 APR 25 2019

32 Affidavit in Support of Search Warrant  
3:19-mj-00177



informed me that MACDERMOTT an active member of the U.S. Army.

As a senior enlisted member, he is a Staff Sergeant at the 1<sup>st</sup> Battalion of the 509 Parachute Infantry Regiment, stationed on Joint Base Elmendorf Richardson (JBER), Anchorage, Alaska. He is married and has two children in his household. The children are as follow: daughter – 12 years old, son – 10 years old.

29. On April 16, 2019, at 1930 hours, I conducted surveillance at 13720 Malaspina Street, Unit A, Eagle River, Alaska 99577, and noticed a red Nissan truck on the drive way. The vehicle's plate number was not readily readable.
30. On April 17, 2019 morning, I conducted surveillance at the parking lot of building 606, where the field Headquarter of the 1<sup>st</sup> Battalion of the 509 Parachute Infantry Regiment located on JBER, and observed similar a red Nissan truck from 13720 Malaspina Street, Unit A, Eagle River, Alaska 99577. The truck's license plate appears to be an Alaska state's plate and reads 'JNM214'.
31. On the same day, I conducted a search in Alaska Department of Public Safety's database for ownership information of the red Nissan truck bearing Alaska plate number 'JNM214'. Search result of the Alaska Department of Public Safety's database reveals the plate is for a red 2011 Nissan truck and registered to MACDERMOTT at 13720 Malaspina, Unit A, Eagle River, Alaska 99577.



APR 25 2019

32. On April 19, 2019, U.S. Army-CID Assistant Special Agent in Charge William Stern confirmed the biographical information of MACDERMOTT's children. They are as follow: son: Caiden Gabriel MACDERMOTT, age 10, and Arielle Jensine Paicaglino MACDERMOTT, age 12.

33. Examination of the child pornography profile image "chrissmith790" uploaded revealed visual depiction as follows:

- a) a prepubescent female (approximately between the ages of three (3) to eight (8) years-old), with clothing from the waist up, holding an adult male's penis in her left hand and her mouth.

**Kik username "chrisschmidt159"**

34. On December 27, 2018, at 21:26 UTC, Kik user "chrisschmidt159" uploaded a profile image in a chat, that was identified by PhotoDNA employed by Kik based on hash information contained in a database with approximately 92,000 child pornography images and corresponding hash information. NCECC forwarded the historical account activity information associated with "chrisschmidt159" to HSI Ottawa due to one of the IP address used, 69.178.7.183, to be located in United States. HSI Ottawa subsequently forwarded the information from NCECC to HSI Anchorage.



APR 25 2019

35. Contained in the forwarded information, was the Kik IP logs for the user "chrisschmidt159.com" which show that for the period December 19, 2018 to December 27, 2018, there were 127 logins into the Kik service. Based on the IP data, the user appears to be using IP masking technology, possibly a virtual private network (VPN) service, when logging into Kik. Using such a tool would manifest in the IP logs as logins from different locations, typically geographically distant, within a short timeframe. Due to the nature of the technology, since VPNs are often configured to be manually activated, the VPN user may not activate it (either the user forgot or for some reason chose not to), or the VPN service is disconnected due to server issues, resulting in the user's true IP being revealed. A review of "chrisschmidt159" IP logs is consistent with the use of an IP masking service. It shows IPs from five geographic countries – the U.S., Denmark, Japan, China, and Taiwan, oftentimes switching countries within minutes and hours of each other. Since a user cannot physically travel this fast, an IP masking service was most likely used. Furthermore, the IP logs show that Kik changes the remote port periodically, with it always increasing in value, in relatively tight increments. There are no instances of remote port overlaps or the port number ever decreasing or there being an unusual gap, e.g. going from a port of 55766 directly to 60000. This is consistent with there being only



APR 25 2019

one installation of the Kik software logging into the service, and not multiple people geographically dispersed using the same Kik account.

36. Of the 127 IP entries, there are 22 originating from Alaska, administered by GCI Communications in Anchorage. The GCI IP addresses were the only ones that fully resolved without issues with Reverse DNS lookup, etc. so there is a high probability that they are the true IP addresses of the Kik user. The email address used for this Kik account is chrischmidt159@gmail.com, and the account username as "chrisschmidt159".

37. Based on the February 22, 2019 Summons return from GCI, the return showed MACDERMOTT to be the sole account holder for internet service since February 2018 and the user of the same IP address for the summoned timeframe of the Kik activities.

38. Examination of the child pornography image "chrisschmidt159" uploaded revealed visual depiction as follows:

- a) a prepubescent female (approximately between the ages of three (3) to eight (8) years-old), naked from thighs up and her vagina penetrated by what appears to be an adult male's penis.

#### CHARACTERISTICS OF CHILD PORNOGRAPHERS

39. My knowledge of preferential sex offenders and their characteristics is based on my experience as an HSI agent, and other training I have



APR 25 2019

received specific to child exploitation crimes and related computer storage. Based upon such training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics of those who possess, view, receive, distribute, and produce child pornography, which may be exhibited in varying combinations:

- (a) Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.
- (b) Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videos, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.



APR 25 2019

- (c) Individuals who have a sexual interest in children or images of children often maintain their collections in a safe, secure and private environment, such as a computer hard drive or separate digital media. In this case, images and videos of child pornography have been distributed through an Internet-based communications service (Kik). Such distribution necessarily requires the possessing of images on a computer, smart phone, tablet, or other Internet-accessible device.
- (d) Evidence of the distribution and possession of child pornography in this case was located in a Kik group. The use of such a group is not uncommon among individuals with an interest in child pornography. Individuals who have a sexual interest in children or images of children may also correspond with and/or meet others to share information and materials, and conceal such correspondence as they do their sexually explicit material. Individuals may often maintain lists of names, e-mail addresses or telephone numbers of individuals with whom they have been in contact, and who share the same interests in child pornography.
- (e) Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by



APR 25 2019

law enforcement officers involved in the investigation of child pornography throughout the world. The result is that individuals may travel with some or all of their collections, and that evidence of an individual's interest in child pornography may be located in their vehicles. This is particularly true given the portable nature of many laptops computers, tablets, and storage devices that allow for easy transport between and individuals home and their ultimate destination.

40. I respectfully submit that there is probable cause to believe that Troy Nicholas MACDERMOTT, who resides at the SUBJECT PREMISES, has distributed child pornography through his cell phone or other Internet-capable portable device, and that evidence of his distribution and possession are likely to be present on his cell phone or device present on his person, as well as on any computers or other digital devices that are present in the SUBJECT PREMISES. I base my conclusion on my training, as well as my investigative experience gained during the execution of previous search warrants related to individuals identified as distributors, receivers, and possessors of child pornography in unrelated investigations. Specifically, that individuals identified as distributors, receivers, and possessors of child pornography are routinely found to be in possession of significant quantities of child pornography, or to have accessed a significant quantity of child pornography, and that this child



APR 25 2019

39 Affidavit in Support of Search Warrant  
3:19-mj-00177



pornography or evidence of it having been accessed is often located on multiple forms of digital devices. In addition, I base this opinion on several facts, to include the characteristics of child pornographers described herein, as well as the investigation described above.

Specifically, those facts include:

- (a) An individual using a Kik account distributed child pornography on December 11 and 27, 2018. Further, the Kik account may have been associated with Troy Nicholas MACDERMOTT, who resides at the SUBJECT PREMISES. This association is made based upon information provided by Canadian authorities, the above-mentioned photograph of MACDERMOTT, publically-available information from MACDERMOTT, military records, and information obtained from State of Alaska records.
- (b) As noted above, Kik is a mobile phone application that allows users to send messages and images and video files through the Internet. I submit that there is probable cause to search the SUBJECT PREMISES for mobile phones and other portable Internet-capable devices, as well as desktop computers, laptop computers, and other digital storage devices and computer equipment. Individuals who distribute, receive, and possess child pornography on mobile devices may back-up those devices to a desktop or laptop computer in order to preserve the contents



APR 25 2019



of their mobile devices, to include their collections, and protect them from loss. By backing up these collections to a desktop or laptop computer, individuals can also use those devices to trade or distribute images or videos from those collections with other collectors through other online platforms.

(c) As mentioned above, users “chrisschmidt159” and “chrissmith790” last known use of Kik occurred on May 30, 2016. I submit that there is probable cause to believe that evidence of “chrisschmidt159” and “chrissmith790” receipt, distribution, and possession of child pornography are likely to remain in the SUBJECT PREMISES and on any mobile devices possessed by MACDERMOTT. As described above, individuals who distribute and possess child pornography are likely to retain their collections for a significant period of time, often exceeding the interval that exists in this case between the Kik activity and the potential execution of a search of the SUBJECT PREMISES and MACDERMOTT. Furthermore, even if deleted from devices located in the SUBJECT PREMISES and from any mobile devices possessed by MACDERMOTT, as described herein, forensic artifacts of the distribution, receipt, and possession of child pornography may remain on devices.



APR 25 2019

## COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

41. Searching digital devices for criminal evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden," erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

42. Computers and other digital communications devices contain volatile memory that contains information only while the device is in a powered on and/or running state. I know that powering off the device may result in the loss of the volatile information. Adding an external evidence storage device will cause minor changes to the state of the computer but will allow for the best effort in fully capturing the state of the running evidence. This capture of information requires technical expertise to ensure the resulting data can be examined by all subsequent investigators. This captured information may include current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys, or other dynamic details relevant to use of the system.



APR 25 2019

43. As further described in Attachment B, this warrant seeks permission to locate in the SUBJECT PREMISES not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computers were used, the purpose of their use, and who used them. Further, as described above and in Attachment B, this application seeks permission to search and seize records that might be found in the SUBJECT PREMISES, in whatever form they are found. Records may be found in the form of computer files on a hard drive or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis of the computer(s) or other electronic storage media seized.

44. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer hard drives can contain other forms of electronic evidence as well. In particular, records of how a computer has been used, the purposes for which it was used, and who has used it are called for by this warrant. As described above, data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word



APR 25 2019

processing file). Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals (e.g., cameras and printers for creating or reproducing images), the attachment of USB flash storage devices, and the times and dates the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information can sometimes be evidence of a crime, or can point toward the existence of evidence in other locations. Evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the evidence described in Attachment B is included within the scope of the warrant.

45. In finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a drive. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge. This software can allow a computer to be used by others. To



APR 25 2019

investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present on the computer, and, if so, whether the presence of that malicious software might explain the presence of other things found on a computer.

46. Law enforcement personnel trained in searching and seizing computer data will seize items of evidentiary value, and transport the same to an appropriate law enforcement laboratory for off-site review. The electronic media will be reviewed for the evidence described in Attachment B in accordance with and as defined by the review protocols described below.
47. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.
48. I know from training and experience that persons trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child exploitation.



APR 25 2019

49. I know from training and experience that files related to the exploitation of children found on computers and other digital communications devices are usually obtained from the Internet or from cellular data networks using software which often leaves files, logs, or file remnants which would tend to show the method of location or creation of the images, search terms used, and the exchange, transfer, distribution, possession, or origin of the files.

50. I know from training and experience that software and hardware can allow people to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connections at the residence.

51. I am familiar with and understand the implications of the Privacy Protection Act (PPA), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the MACDERMOTT or SUBJECT PREMISES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

52. I know from training and experience that computers or other digital devices used to access the Internet usually contain files, logs, or file remnants which would tend to show ownership and use of the device,



**APR 25 2019**

46

Affidavit in Support of Search Warrant

3:19-mj-00177

ownership and use of any external devices that had been attached to the computer or other digital devices, as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

53. I know from training and experience that digital crime scenes usually include items or digital information that would tend to establish ownership or use of digital devices and Internet access equipment and ownership or use of any Internet service or digital cellular service accounts used to participate in the exchange, receipt, possession, collection or distribution of child pornography.

#### **SPECIFIC METHODS OF SEARCHING FOR DIGITAL EVIDENCE**

##### *Access to Locked Apple Devices Located at the Premises*

54. When searching MACDERMOTT and the SUBJECT PREMISES, it is possible that Apple brand devices, such as iPads or iPhones, will be found. I know this to be a likelihood because, as previously mentioned, the Kik results indicate that the device registered to the Kik account with the username "chrisschmidt159" and "chrissmith790" was an iPhone. The relevant information provided by Kik Interactive to Canadian authorities which indicates this fact is as follows:

a) For "chrissmidt159"

(2018-12-19 17:05:38 UTC REGISTRATION\_CLIENT\_INFO device-type=iphone); and



APR 25 2019

47 Affidavit in Support of Search Warrant  
3:19-mj-00177

b) For “chrissmith790”

(2018-12-19 17:05:38 UTC REGISTRATION\_CLIENT\_INFO device-type=iphone); and

55. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) or facial recognition in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID or Face ID, depending on the model of the Apple device.

56. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. Similarly, Face ID allows a user to unlock the iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user’s face. Face ID confirms attention by detecting the direction of the user’s gaze, then uses neural networks for matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user’s appearance, and carefully safeguards the privacy and security of the user’s biometric data.

57. In my training and experience, users of Apple devices that offer Touch ID and Face ID often enable it because it is considered to be a more convenient way to unlock the



APR 25 2019



device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

58. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) five unsuccessful attempts to unlock the device via Touch ID are made; (4) when more than 48 hours has passed since the last time the device was unlocked; and (5) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days.

Similarly, the user's face cannot be used to unlock a device that has Face ID enabled, and a passcode or password must be used in these circumstances: (1) the device has just been turned on or restarted; (2) the device has not been unlocked for more than 48 hours; (3) the passcode hasn't been used to unlock the device in the last 156 hours (six and a half days) and Face ID has not unlocked the device in the last 4 hours; (4) the device has received a remote lock command; (5) after five unsuccessful attempts to match a face; (6) after initiating power off/Emergency SOS by pressing and holding either volume button and the side button simultaneously for 2 seconds. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID or Face ID exists only for a short time.

59. The passcode or password that would unlock the Apple device found during the search of the Premises is not known to law enforcement. Thus, it will likely be



APR 25 2019

necessary to press the fingers of the users of the Apple device found during the search of the Premises to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Similarly, it will likely be necessary to have the user remain still and look, with eyes open, at the front-facing camera (the Face ID sensor) of the of the Apple device found during the search of the Premises in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the users or Face ID with the use of the user's face is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

60. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints or face are among those that will unlock the device via Touch ID or Face ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the Premises to press their fingers against the Touch ID sensor or look at the Face ID sensor of the locked Apple device found during the



APR 25 2019

50 Affidavit in Support of Search Warrant  
3:19-mj-00177

search of the Premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID or Face ID. Based on these facts and my training and experience, it is likely that MACDERMOTT is the sole user of the device(s) and thus that MACDERMOTT fingerprints or face are among those that are able to unlock the device via Touch ID or Face ID.

61. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the Premises as described above within the five attempts permitted by Touch ID or Face ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

62. Prior to compelling the facial recognition or fingerprint of Troy Nicholas MACDERMOTT onto any device located at the SUBJECT PREMISES and on his person, law enforcement will make efforts to identify those with lawful access to the device, by examining the location in which the device was found, the items with which the device was co-mingled, or any plainly visible labels or indicators on the exterior of the device.

63. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of the above-named individuals found at the Premises to the Touch ID sensor of the device(s), or to instruct the user to remain still, with eyes looking forward at the Face ID sensor of the device(s), such as an iPhone or an iPad, found at




APR 25 2019

the Premises for the purpose of attempting to unlock the device(s) via Touch ID or Face ID in order to search the contents as authorized by this warrant.

***Authority to Search SUBJECT PREMISES and MACDERMOTT***

64. Because of the above characteristics about individuals who transport, possess, receive, and access with intent to view child pornography, this warrant seeks authority to search both the SUBJECT PREMISES, to include vehicles at the SUBJECT PREMISES, and the person Troy Nicholas MACDERMOTT. Law enforcement intends to execute this search at a time when Troy Nicholas MACDERMOTT is present in the SUBJECT PREMISES. During the search of Troy Nicholas MACDERMOTT, law enforcement intends to seize any child pornography, and any tablets, smart phones, thumb drives, SD cards, or other digital devices upon which child pornography or evidence of the transportation, possession, receipt, and accessing with the intent to view can be located. The search of the person of Troy Nicholas MACDERMOTT and any vehicles at the SUBJECT PREMISES is warranted in this case because the trading of child pornography appears to have occurred through the Kik application, which is most frequently accessed through a mobile phone or tablet, devices that are typically carried on a person. I seek this authority because of the ubiquity of digital devices in modern society, and the ease with which contraband can be transported, possessed received,

  
APR 25 2019

and accessed with the intent view on those devices. Tablets and smart phones can easily access the Internet from any location with cell or wi-fi service. Once on the Internet, these devices can navigate to file-sharing sites. These images can be easily saved onto those portable digital devices, as well as onto thumb drives and SD cards that might be connected to those devices. Absent the authority to search the person of Troy Nicholas MACDERMOTT, these items may escape detection.

65. I am seeking authority to search for, among other things, items containing digital data, more particularly described in Attachment B. Consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

66. The search of a computer hard drive or other computer storage medium is a time-consuming manual process often requiring months of work. The process can take a significant amount time for a number of reasons, including the complexity of computer systems, the multiple devices upon which computing can take place, the tremendous storage capacity of



APR 25 2019

modern day computers, and the use of encryption or wiping software. As explained above, modern day computers and storage devices are capable of holding massive quantities of child pornography, and the volume of evidence seized in these cases can be immense. I am aware of cases in which individuals have possessed thousands of images of child pornography on multiple computers, hard drives, and other storage media. I know from my training and experience that a review of such quantities of evidence can take a significant amount of time. Second, there is a limited pool of personnel capable of conducting a forensic examination. Third, in some instances an individual may utilize encryption software or other publically-available techniques such as wiping software to hide their collections of child pornography. Forensic tools are available to circumvent some of these techniques; however, these tools may require a significant allocation of resources and a substantial period of time.

67. Some or all of the following search methods may be used to conduct the forensic search in this case. These methods are not listed in any particular order, nor is their listings in this affidavit a representation that they will be used in this particular case:

(a) *Keyword Searches*: I know that computer forensic utilities provide the capability for a user to search for specific key words that may exist on a piece of digital media. I intend to use specific keywords known to be related to either the subject's



APR 25 2019

illicit internet activities or child pornography. As it concerns child pornography, examples of such keywords include, but are not limited to "preteen," "hussyfan," and "r@ygold." Those keyword searches will indicate files and other areas of the hard drive that need to be further reviewed to determine if those areas contain relevant data. A list of keywords utilized will be maintained with the records of the forensic examination.

(b) *Data Carving*: I know that, as previously mentioned, data residue may be left in the "free," "unallocated," or "slack" space of a computer hard drive, that is, the space not currently used by active files. I further know that, as previously mentioned, many operating systems utilize temporary storage often referred to as "swap space" on the hard drive to store contents from main system memory. Such unallocated and swap space may contain the residue of files that can be carved out, often in an automated or semi-automated fashion. I intend to use forensic tools to carve out files, in particular, image files such as JPEG and GIF files. The mere act of carving out such files, makes those files available for further relevancy checks, such as keyword searches (explained above) and hash value comparisons (explained below).



APR 25 2019

(c) *Hash Value Comparisons*: I know that computer forensic utilities provide the capability to utilize a function known as a hash algorithm. A hash algorithm uses a mathematical formula to analyze the data composing a file, and to generate a unique value or "fingerprint" for that file. The act of hashing a piece of data does not reveal to an investigator any information about the contents of that data. However, I know that computer forensic applications often contain databases of known hash values for files. Some of those files are "ignorable," which enables other forensic processes to ignore files (such as the Windows operating system) that are not evidentiary in nature. Some of the files are "alert" files, such as the Child Victim Identification Program (CVIP) hash set that contains hash values for a small subset of the identified picture and video files for known victims of child pornography. CVIP alert files notify an examiner that a file appears to contain known depictions of child pornography. I seek permission to utilize automated hash value comparisons to both exclude irrelevant files, and to locate known child pornography files. Hash value comparisons are useful, but not definitive, as even a single-bit change to a file will alter the hash value for the file. The forensic review team does not intend to rely solely on hash value comparisons, but



APR 25 2019

56 Affidavit in Support of Search Warrant  
3:19-mj-00177



intends to utilize them in order to assist with identifying relevant evidence. The use of this search method is intended to narrow the search. A search of known hash values, however, will not be used exclusively. I know that when previously identified images of child pornography are found on a target's computer, typically there are many more images of child pornography with unknown hash values. Using a hash value search method exclusively would not uncover these images as well as other evidence authorized by this warrant and described in Attachment B.

(d) *Opening Container Files, Encrypted Volumes, and Embedded*

*Files:* I know that relevant data may be compressed, encrypted, or otherwise embedded in other files or volumes. It is often not possible through any automated process to examine the contents of such containers without opening them, just as it is not possible to examine the contents of a locked safe without first opening the safe. In the event that compressed, encrypted, or otherwise embedded files or volumes may exist on the seized items, I intend to use sophisticated forensic tools to attempt to open any such container files that may reasonably contain evidence of child pornography.



APR 25 2019

- (e) *File Header / Extension Checks*: I know that individuals involved in illegal activities on a computer often change the extension of a file (such as .jpg) to some other incompatible extension (such as .txt) in order to disguise files from casual observers. The extension of a file, however, is not necessarily linked to the "header" of a file, which is a unique marking imbedded automatically in many types of files. By comparing the extension of a file with the "header information" of a file, it is possible to detect attempts to disguise evidence of illegal activities. Such a comparison can be made in an automated process by computer forensic tools. I intend to run an automated header comparison to detect such efforts, and intend to review any such files that reasonably may contain evidence of child pornography.
- (f) *Thumbnail / Image Views*: Although hash value comparisons can positively identify known child pornography depictions, a negative hash value comparison does not exclude an image from suspicion. There is no known alternative for visually inspecting each image file. I therefore intend to examine at least a thumbnail image of each image file on the digital media whether "live," "data carved," or identified by header.



APR 25 2019

(g) *Registry / Log File Checks*: I know that it is necessary in any criminal case to establish not only that a crime has occurred, but also to establish what person committed that crime. Operating systems and computer programs often maintain various administrative files such as logs that contain information about user activities at certain times. In the Windows operating system, for example, some of these files are collectively referred to as "the registry". Such files contain specific information about users, often including e-mail addresses used, passwords stored, and programs executed by a particular user. These files may also contain evidence regarding storage devices that have been connected to a computer at some time. Multiple backup copies of such files may exist on a single computer. I intend to examine these files to attempt to establish the identity of any user involved in the receipt, possession, distribution, and transportation of child pornography, and to establish methods (such as software used) and dates of this activity.

(h) *Metadata / Alternative Data Streams*: I know that many file types, operating systems, and file systems have mechanisms for storing information that is not immediately visible to the end user without some effort. Metadata, as described earlier, may identify the camera that produced a particular image, as well as



APR 25 2019

the date, time, and location the image was taken. Some file systems for computers also permit the storage of alternate data streams, whereby a file such as a text file may hide an image file that would not be immediately visible to an end user without some action taken. I know that both metadata and alternative data streams may contain information that may be relevant to child pornography offenses. Metadata and alternative data streams are often identified and processed automatically by computer forensic utilities. I intend to review any such data that is flagged by any process above as being relevant to the receipt, possession, distribution, and transportation of child pornography.

68. With rare exception, the above-listed search techniques will not be performed on original digital evidence. Instead, I know that the first priority of a digital evidence forensic examination is the preservation of all data seized. As such, original digital media will be, wherever possible, copied, or "imaged," prior to the start of any search for evidence. The copy will be authenticated digitally as described in the paragraph below.

69. I know that a digital forensic image is the best possible copy that can be obtained for a piece of digital media. Forensic imaging tools make an exact copy of every accessible piece of data on the original digital media.

In general, the data contained on the original media is run through a



APR 25 2019

hashing algorithm as described above, and a hash value for the entire device is generated. Upon completion of the imaging process, the same hash algorithm is run on the imaged copy to insure the copy is an exact duplicate of the original.

70. Criminal Procedure Rule 41 specifically states “The officer may retain a copy of the electronically stored information that was seized or copied.” Fed. R. Crim. P. 41 (f)(1)(B). Moreover, upon identification of contraband, the item is subject to forfeiture, and the owner has a reduced expectation of privacy in those seized devices. Consequently, should a seized device be found during the authorized forensic review to contain child pornography, it will be retained by the United States, and may be searched without further authorization of the Court for the evidence described in Attachment B. Such a later search may be required for the following reasons:

- (a) Should the execution of the warrant uncover data that may later need to be introduced into evidence during a trial or other proceeding, the authenticity and the integrity of the evidence and the government's forensic methodology may be contested issues. Retaining copies of seized storage media may be required to prove these facts.
- (b) Returning the original storage medium to its owner will not allow for the preservation of that evidence. Even routine use



APR 25 2019

may forever change the data it contains, alter system access times, or eliminate data stored on it.

- (c) Because the investigation is not yet complete, it is not possible to predict all possible defendants against whom evidence found on the storage medium might be used. That evidence might be used against persons who have no possessory interest in the storage media, or against persons yet unknown. Those defendants might be entitled to a copy of the complete storage media in discovery. Retention of a complete image assures that it will be available to all parties, including those known now and those later identified.
- (d) The act of destroying or returning storage medium could create an opportunity for a defendant to claim, falsely, that the destroyed or returned storage medium contained evidence favorable to him. Maintaining a copy of the storage medium would permit the government, through an additional warrant if necessary, to investigate such a claim.
- (e) Similarly, should a defendant suggest an explanation for the presence of evidence on storage medium or some defense, it may be necessary to investigate such an explanation or defense by, among other things, re-examining the storage medium with that explanation or defense in mind. This may require an additional



APR 25 2019

examination of the storage medium for evidence that is described in Attachment B, but was not properly identified and segregated previously.

71. In the event that a piece of digital media is found not to be (a) an instrumentality of the offense, (b) a fruit of the criminal activity, (c) contraband, or (d) evidence of the offenses specified herein, it will be returned as quickly as possible.

72. As it concerns computer evidence, this warrant does not contain a limitation on the locations within a digital device that may be searched, or the types of data that may be seized from those locations. This is so for multiple reasons, each of which has been addressed in greater detail above. First, as noted above, individuals who receive and collect child pornography have been documented to retain their collections for years. When a collection consists of digital images, that data may remain on a computer indefinitely. The indefinite storage of digital evidence can occur even if the computer is not actively used and the files are deleted. Second, sophisticated computer users are able to manipulate the data on their computers to hide contraband or alter information associated with a contraband file. Without the ability to examine all parts of the computer, and all files located therein, it may be impossible to know for certain whether or not contraband is present. Third, individuals may use multiple platforms within their digital devices to acquire images, such as



APR 25 2019

open searches on the Internet (i.e. Google), Internet-based file-sharing services, and other third-party applications ("Apps"). Therefore, it is necessary in any search for child pornography to be able to examine the entirety of the computer without limitation to date ranges, programs, or file types, in order to be able to ensure that each of these platforms have been examined.

### SEALING REQUEST

73. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that prematurely disclosing this information could result in the destruction of evidence and have an adverse impact on officer safety. Furthermore, the items and information to be seized are relevant to an ongoing investigation involving residents of the SUBJECT PREMISES. Disclosure of the contents of this application and related documents may have a significant and negative impact on the continuing investigation and/or may severely jeopardize its effectiveness by allowing individuals at the SUBJECT PREMISES and MACDERMOTT to destroy or hide evidence.

### CONCLUSION




APR 25 2019



74. Based upon the information above, your affiant submits that there is probable cause to believe that violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) have been committed, that the items described in Attachment B are evidence, fruits, and instrumentalities of those violations and that the items described in Attachment B are likely to be found at the premises described in Attachment A.

75. I request that the Court issue a warrant authorizing a search of the SUBJECT PREMISE and Troy Nicholas MACDERMOTT, that is described in Attachment A, for the items described in Attachment B.

  
Yi-Lin Lee  
Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me this  
25<sup>th</sup> day of April, 2019

/S/ MATTHEW M. SCOBLE  
U.S. MAGISTRATE JUDGE  
SIGNATURE REDACTED

NAME

United States Magistrate Judge  
District of Alaska  
Anchorage, Alaska

